Journal of Academic Librarianship, 1990, Vol. 16, No. 5, p. 296-301.
ISSN: 0099-1333
http://www.sciencedirect.com/science/journal/00991333
http://proxy.lib.ohio-state.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=9705180776&site=ehost-live

Internal Control, Auditing, and the Automated Acquisitions System

by Carol Pitts Hawks

As automated acquisitions systems become more prevalent, the importance of the issues and procedures involved in their auditing increases. This paper examines those issues and procedures, clarifies the audit process, and identifies internal controls as they relate to the automated acquisitions system. General control mechanisms, such as access to equipment, and application controls, such as segregation of functions, are described.

The Ohio State University Libraries (OSUL) were notified in the summer of 1987 that the University's Internal Audit Department would conduct an audit of the purchasing and payables functions of the Acquisition Department. The department is one of several satellite accounts payable operations on campus authorized to issue purchase orders in the name of the University and to maintain internal encumbrances not reflected individually at the university level until payment. In addition, checks are returned to the department for verification and mailing rather than being mailed directly from the University's Accounts Payable Department. This authority, which carries with it the obligation to maintain records providing complete documentation for fiscal transactions, has greatly improved the Acquisition Department's ability to effect prompt payment and resolve problems expeditiously. And, because the department knows when and if checks have been written and mailed, problems are easier to resolve.

It was very important to preserving the satellite payable status of the Acquisition Department that the internal controls examined in the audit be found adequate. This was the first comprehensive audit that the department had undergone since the implementation of OSUL's automated acquisitions system, INNOVACQ, in 1984. (The previous audit report in 1982 found the internal controls in the manual system to be adequate but recommended additional electronic data processing [EDP] support.) This paper examines the issues and procedures involved in auditing an automated acquisitions system, clarifies the audit process, and identifies internal controls as they relate to the automated acquisitions system, based on this initial internal audit of the INNOVACQ system at OSUL.

Automated Acquisitions Systems

Automated acquisitions systems are used in many libraries. Some were implemented as stand-alone systems to rescue a crippled manual system; others were acquired as one module of an

integrated library system. It is common practice in libraries to computerize as many operations as possible, and, less commonly, to simply assume that computerized systems have adequate internal control features—i.e., mechanisms to track, count, and report on system usage. If systems designers are not specialists in developing internal controls, however, the necessary controls may *not* have been built into the system; and adding controls to an extant system is usually costly and sometimes impossible.[1] Therefore, it is imperative that the acquisitions librarian responsible for implementing an automated acquisitions system understand the principles of internal control and auditing to ensure a well-designed, properly implemented system.

The fund accounting component is the most critical aspect of an automated acquisitions system since it "provides for the control of the library's materials budgets by recording and monitoring the allocations, expenditures and balances of each budget category."[2] In a manual system, internal accounting control to prevent or detect errors, irregularities, or fraud relies heavily on factors such as judgment, acceptance of responsibility, and segregation of functions. Automation reduces the extent of control based on human judgment and alertness. Instead, the computer often provides alternative controls that can be more effective than manual controls,[3] even while creating areas and opportunities for problems to occur. Most libraries are aware of the controls placed upon them by their parent institution in the areas of purchasing procedures and invoice processing. However, most librarians may not be as well-informed about auditing standards and expectations, particularly as they apply to automated systems.

Audits and Audit Trails

A successful audit is contingent upon the availability of audit trails. In an automated acquisitions system, an audit trail permits an auditor (1) to identify each step in the acquisitions process, from placing the initial order through receiving and housing the materials, or (2) to work backwards, tracing the actual materials back to the original purchase orders. For example, system-generated expenditure reports on a federal grant would allow an auditor to evaluate whether the purchase had been authorized by the principal investigator, whether the order, receiving, and invoicing documents for the title were in order, and whether the total expenditure for the account was supported by documentation for each purchase. In addition, audit trails provide internal checks and balances in the day-to-day operations of the acquisition department. For example, if the department has requested payment of an invoice but the vendor has not received a check, the audit trail can identify when payment was requested and provide the name and address of the vendor used, thus, providing a tracking mechanism.

Accounting standards are established for both private- and public-sector organizations in the U.S. by the Financial Accounting Standards Board (FASB). In addition to the FASB, the American Institute of Certified Public Accountants (AICPA) issues accounting guidelines which, although they are not binding, are indicative of the most favored accounting practices. Adherence to standards and guidelines facilitates the correct analysis of summarized results, thus avoiding difficulties in interpretation and comparison of management information.[4]

Benefits of an Audit

The benefits of an audit to the library and its acquisition department are substantial. As a management tool, the audit can provide a great deal of information about the library's automated

system. The auditor can provide an unbiased analysis of the strengths and weaknesses of the system, suggest improvements in the accuracy and reliability of data, and build confidence in the integrity of the system.

Although there are several types of audits and auditors, this article's focus is on the performance audit as conducted by an internal auditor. The internal auditor is an employee of the library's parent organization and operates independently within the organization with no authority over or responsibility for routine accounting activities. The auditor evaluates the system for accuracy, consistency, and compliance with the organization's purchasing and accounting policies.[5] If the audit reveals deficiencies or weaknesses in the control process, they are reported to management with recommendations for corrective action.[6]

Preparation for the Audit

Regardless of whether an audit is imminent or only anticipated at some point in the future, the library's best approach is to be prepared. Early evaluation of a system will confirm that the system is a reliable one or identify problem areas that can be rectified prior to an actual audit. Problems should be addressed before they become too large to resolve simply.[7]

One area to consider in conducting this evaluation is to identify and examine the informal system that exists behind the formal system. Informal systems weaken controls and may provide the opportunity for fraud. For example, the password structure in the system may limit access to the check writing function to the accounting supervisor. However, due to the supervisor's frequent absences, the required password has been given to the ordering supervisor, who produces checks in the absence of the accounting supervisor. On the surface the control mechanism is intact, but in reality the integrity of the control has been compromised.

The final precaution that should be taken is preparation of records retention schedules. Most organizations have a system of records management that regulates which report must be retained and for what length of time. This step is of particular importance when automated systems are introduced because electronic as well as paper files must have retention schedules. If a library has evaluated its own system, corrected problems identified, examined the informal procedures, and established records retention schedules, an internal audit can be approached with confidence.

The Audit Process

Once the decision has been made to audit the library, the auditor must be provided with an overall understanding of the structure of manual and automated systems, the extent to which each is used, and an overview of the work flow. The importance of the librarian's role during this review phase cannot be overemphasized because this phase forms the basis for planning the remainder of the audit. Libraries face a special challenge in this area because of the inherent complexity of acquiring library materials. Therefore, it is imperative that the acquisition department expend the time and effort required to ensure that the auditor fully understands the work flow and routines within the system.

The auditor's primary concern will be whether the controls built into the system are being used properly. Evaluation of the controls will involve questions such as: Were the necessary procedures performed? How were they performed? By whom were they performed? [8] For exam-

ple, in an automated acquisitions system the auditor would explore questions such as:

- Did the appropriate person sign the voucher for payment?
- Did the subject selector initial the request for purchase?
- Did the system verify the password of the person who signed on to the system to process the invoice?
- Were passwords made available to and used by inappropriate personnel?

To answer these questions, a sample of transactions will be randomly selected from the entire period covered by the audit. (The size of the sample selected is an excellent indicator of the auditor's initial confidence in the system.) Once the auditor has identified the sample, the library will be asked to assemble the appropriate documentation to support the evaluation. The auditor will examine and evaluate the documentation, and prepare a written report. This report will include detailed audit findings and recommendations that will be sent to the library administration and other appropriate university administrators.

OSUL's Audit

In the library setting, the audit process will often mirror the process that occurred in 1987/88 at OSUL. An auditor from the Internal Audit Department was assigned responsibility for the audit of the Acquisition Department. The auditor met with the department head and the division heads within the department, and a considerable amount of time was spent with the manager of the INNOVACQ system to gain an understanding of the control mechanisms within the system. In addition, the auditor was encouraged to contact Innovative Interfaces (the vendor for INNOVACQ) directly for clarification of issues that the manager could not provide. Job descriptions, procedures, and system documentation were provided to the auditor. In addition, he requested that charts identifying password authorization be constructed. The auditor developed flowcharts of the acquisitions process and consulted with the division heads to modify those charts as appropriate.

Once the review phase was completed, the auditor selected a sample of 35 accounting entries from various library accounts included in the University's Accounts Payable ledgers. These entries did not represent single purchases but rather single invoices. Each order on the payment record had to be documented. Invoices were retrieved, records for individual titles were located on INNOVACQ and printed, and the online catalog entries were printed. The availability of catalog records provides a secondary control mechanism for library materials—i.e., many other purchases, such as paper, are consumable and cannot be physically observed by the time -an audit is conducted. The INNOVACQ records provide the evidence of order, receipt, and payment. The catalog provides evidence that the actual item has been added to the collection, although in several cases, the material under consideration in the audit had not yet been cataloged. Some uncataloged items were located in the pre-cataloging area and physically examined by the auditor. Uncataloged special collection materials were retrieved and the auditor visited various campus libraries to see the physical items. The auditor evaluated all of the documentation provided and calculated balances on the invoices.

The auditor then prepared a written report that was submitted to the library administration in draft form. He subsequently met with the Head of the Acquisition Department, the Assistant Director for Technical Services, and the Director of Libraries to clarify issues and rectify

misconceptions. The final report was sent to the library administration and appropriate university administrators. The library responded to the report, indicating the recommendations that had been or would be implemented, and expressing an objection to one recommendation. For example, the audit recommended the establishment of a signature file much like those found in banks. Each collection manager's signature and initials are recorded against the funds for which they are authorized to initiate orders. This recommendation was immediately implemented by OSUL.

Internal audit conducted a follow-up visit in the summer of 1988 to assess compliance with the audit report. Their findings from this visit were reported in the same manner.

Internal Controls

The internal control mechanisms within a system form the focal point of an audit. Ideally, the value of an internal control mechanism lies in its ability to *prevent* errors, fraud, or waste rather than to merely detect them. However, some preventive controls may not be cost beneficial.[9] For example, having every order authorized by a high-level staff member may not be cost effective, but it may be practical to require that orders over $500 have such additional authorization.

Detection controls can be sufficient if they occur on a timely basis in the normal course of operations. It is also common for system designers to build in redundant or compensating controls that counteract ineffectiveness or weakness in the primary control. For example, a system may have no mechanism to alert an order entry clerk that a particular fund has no available balance (primary control). At a later point, when the system attempts to encumber the funds, the order will be rejected (secondary control). Redundant controls should also be governed by cost/ benefit considerations such as the risk exposure from a potential error. This ability of one control to compensate for another is of particular interest to the auditor.[10] The following is an example of compensating controls. At OSUL only specific employees in the Acquisition Department are authorized to issue purchase orders for library materials. These purchase orders have, in turn, been initiated and initialed by the selector responsible for the fund. Further, orders over a certain dollar amount must be authorized by the Head of the Acquisition Department and/or the Collection Development Officer.

General Control Mechanisms

Controls for automated systems are divided into two principal categories: general controls that apply to all aspects of the system and application controls that relate to the specific subsystems. General controls, which are typically evaluated by the auditor first, can be divided into two types: controls that separate computer data processing functions (following an organizational plan) and controls over access to equipment and data files.[11]

Segregating functions. The organizational plan is primarily concerned with the segregation of functions between systems staff and users. Systems staff maintain and service the physical computers; users are the staff members who perform acquisitions tasks on the system such as ordering and invoicing. The type of system the library owns will play an integral part in the segregation of those who maintain it and those who use it. Large integrated library systems, such as NOTIS or Geac, often demand the attention of full-time systems staff members located in the library or in a centralized computer center. These staff have no role in the application functions of

the system and rarely have the familiarity with applications programs to complete or conceal fraudulent activities. On the other hand, a stand-alone system in a small organization or one such as INNOVACQ, which requires no environmental controls, is often housed in the acquisition department itself. The systems staff are also typically the users of that system. One method for establishing some segregation of duties is to assign responsibility for the maintenance of the system to an employee who does not enter data. For example, without appropriate controls an employee who has access to computer records could enter fictitious transactions causing shipment of goods or payment of invoices to unauthorized individuals.

Limiting electronic access. Controls over access to data files and equipment play a larger role in the audit process than most libraries would expect. The ability to control access to datafiles and to control enhancements to the software by the vendor is a critical area of concern for an auditor. The audit of the OSUL resulted in recommendations in this area.

Innovative Interfaces, Inc. (III) maintains, troubleshoots, and eliminates bugs from the INNOVACQ system by dialing into a modem attached to the system. This modem was accessible to III 24 hours a day. This was particularly useful given the difference in time zones between III (Pacific) and OSUL (Eastern). Nevertheless, the internal auditor determined that this allowed access to the system by III without the knowledge of the department. As a result, the modem is disconnected when III is not dialed in to address a specific problem. When III wishes to access the system, permission must be obtained by logging the request, giving the approximate time required, and stating the service to be performed. If the request is approved, OSUL activates the modem. Other automated systems, such as Geac, accommodate this control mechanism by maintaining a computer log within the system which documents the access automatically. Geac carries this a step further by requiring its own staff to document what occurred before exiting the system.

Access can be further controlled by the use of identification techniques such as passwords to access online programs and data. Some systems, such as INNOVACQ, allow access to search functions without the use of a password. Other systems, such as Geac, carry this security to greater lengths by requiring password authorization for access to *any* system function. Dial access from remote locations also poses a threat to security. At OSUL, access to INNOVACQ from branch libraries was considered essential for problem resolution. Fortunately, the INNOVACQ dial access feature can be restricted to permit search access only. Systems which permit update functions from remote locations can ensure additional security by monitoring unsuccessful attempts to access the system. Stettler, writing on auditing principles in a systems-based environment, states:

> Repeated attempts to access a file with incorrect passwords could indicate that someone is trying to guess the password or to exhaust all the combinations of characters until one works. Some password security procedures can also shut down any terminal that logs repeated attempts to use incorrect passwords or to use certain instructions.[12]

Limiting physical access. Reports of intentional abuse of hardware and destruction of data have increased significantly in the past few years. As a result, the computer must be made secure by physically limiting access to authorized persons. Mainframe and minicomputers usually require climate-controlled facilities that maintain and monitor temperature and humidity. As a result, separate computer rooms are frequently constructed to house this hardware. In this case, access

can be restricted by the use of locks, guards, alarms, and identification badges. In addition, common sense dictates that the computer's location should not be in a public area or near any unsupervised entrances. For example, at the University of Houston Libraries, the computer is located in an unmarked room accessible only through a restricted area staffed by a receptionist during working hours and two sets of locked doors after hours. Smaller microcomputer systems pose more of a challenge since they generally do not require a controlled environment. In such instances, it may be difficult to limit physical access to the computer. Locking keyboards are available but, at the very least, the system should be in a restricted traffic area that can be secured after hours.

"Controls over access to datafields and equipment play a larger role in the audit process than most libraries would expect. The ability to control access to datafiles and to control enhancements to the software by the vendor is a critical area of concern for an auditor."

If the auditor's review of these general controls indicates that the controls are reliable, s/he will proceed with testing the effectiveness of the application controls.

Application Control Mechanisms

Application controls are concerned with the specific computer applications and software used to perform the functions of the system. There are three primary application controls of importance in the automated acquisitions system: segregating functions, authorizing transactions, and recording transactions.[13]

Segregating functions. The segregation of functions is one of the critical elements of application control. The philosophy inherent in this control is that, if appropriate segregation is maintained, the only way theft or fraud can occur successfully is through collusion. Collusion requires two or more employees to work together to commit theft which could not have been completed by only one of them. Obviously, the larger the number of people required to commit fraud, the greater the risk of detection. Additionally, this control ensures that no single employee is placed in a position to perpetuate and conceal errors while performing regularly assigned duties. Segregation can be effectively implemented by separating three principal activities: authorization of transactions, custody of assets, and accounting for transactions. Adequate segregation is more difficult to achieve in smaller organizations, but as long as the organization or department has at least three employees, segregation can be maintained.

In the library acquisitions area, segregation begins at the very earliest stages. Purchase order preparation (authorization) must be separate from receiving (custody), and both must be independent of invoice processing and payment (accounting). In many libraries, the process concludes with invoice processing. However, in organizations where checks are prepared in or mailed from the acquisition department, the person responsible for check preparation should not be the person who approves vouchers for payment.

Generally, appropriate segregation of duties is obtained when the work of one employee is checked by another employee or another department. This does not imply that work should be

double-checked, but that subsequent steps in the workflow should verify previous steps.[14] For example, when books are received, someone verifies receipt, updates the record in the system, and initials or signs the invoice. This certifies that payment can be made. The invoice can then be compared to the online order and receipt information to document the entire transaction. This documentation provides the voucher or authority for payment, which is sent to the organization's accounts payable department where the checks are written.

Using passwords. Automated acquisitions systems have dramatically affected the concept of segregation of functions. In her book on internal accounting controls, Wallace warns:

> Documentation that was typically segregated in a manual system through the assignment of responsibilities to different individuals is all processed through a centralized electronic data processing (EDP) system. This combination of duties poses a potentially high risk to control and must be explicitly evaluated and, where possible, compensated for through alternative control procedures.[15]

The most common, and effective, compensating control is the use of passwords for access to online programs and the database. Specific applications functions or access can be limited by a set of parameters that are job defined. For example, a receiving clerk would be able to receive material and update fields as necessary, but the ability to perform other functions, such as authorizing orders, issuing invoices, or adjusting budgets, would be restricted. In fact, the menu commands to access these areas may not even appear on the receiving clerk's monitor.

Passwords can be employed to control the following tasks:

- access the system,
- access high-, medium-, or low-security files or data,
- read data,
- read and modify data,
- add new data, and
- delete data.

For example, in most cases subject selectors are permitted full-display access to the system with read-only options—i.e., they can view all information but cannot add to, modify, or delete it. Similarly, data entry clerks are allowed access to input order requests, but they may be restricted to entering orders valued at under $250. Medium-security access may be granted to the ordering supervisor, who could authorize orders over $250 but less than $500, and high-security access may be given to the department head, who could authorize orders over $500.

Passwords are effective only if certain conditions are met. The password must be kept secret, should not be written down, and should not be given to another user. Most systems now suppress or camouflage the printing of passwords when entered on the terminal to increase the security of the password. Passwords should be difficult to guess, e.g., names, birthdays, or Social Security numbers should not be used. In fact, passwords randomly generated by the system are the most secure. Passwords should be changed periodically, particularly whenever a person changes positions or whenever there is any suspicion that a breach in security may have occurred.

The password structure will be of great interest to an internal auditor. One of the most effective means for controlling and monitoring the use of passwords is a matrix document which correlates users with appropriate functions. A matrix or chart makes it possible to readily spot

authorization for incompatible functions and provides the department head and the auditor with the information on who has authority to do what.

Authorizing transactions. The second application control verifies that all transactions have been properly authorized. In most libraries, the acquisitions librarian authorizes the purchase of library materials. Other individuals, such as subject selectors, are called upon to initiate requests for purchase, but the ultimate responsibility for issuing purchase orders resides in the acquisition department. Although institutional regulations may limit the success with which this can be accomplished, the authority to make expenditures should be placed as close as possible to the order point.[16] Nevertheless, it may be possible to use a closely held signature stamp or delegate this responsibility whenever possible.

The authorization process occurs throughout the acquisitions routine. For example, the subject selector determines that a particular book is needed, resulting in the preparation of a purchase request. This request authorizes the acquisition department to order the title on a particular fund that is assigned to the selector. The purchase order issued by the acquisition department in turn authorizes the vendor to ship the material, the receiving division to accept it, and the accounting division to initiate a request for payment. Evidence (such as a signature or initials) must be present at each stage to verify that the appropriate documentation and checking procedures have been completed. To be viable, authorization levels should be realistic and consistent with the importance of the issue and the responsibilities of the employees concerned.[17]

Computers are well suited to monitor and report instances where authorization is required or has not been provided. At the earliest point, the system's password structure and other controls limit access. In addition, most systems keep an electronic log of who has performed what functions. For example, the clerk who is authorized to process requests from the selector for art history may be confined to entering only such orders, and the clerk's initials may appear on each order record, just as the invoicing clerk's initials may be added to each payment record.

The receiving data recorded in the system will be governed by the computer's internal clock and cannot be adjusted or overridden. Systems can also set limits on fund balances (blocking the placement of an order if the balance of a fund falls below a certain level) and generate "exception reports" to identify purchases over a specific amount that require further authorization.

Unfortunately, library acquisition departments typically make one critical mistake in this authorization process: they fail to formalize the sequence of authorization signatures. This procedure is such an integral part of the acquisitions process that it may simply be understood by all those involved and never documented. Alley and Cargill stress that "a policy spelling out the lines of authority and responsibility is essential to good management."[18] In addition, it is a critical factor in an internal audit. The authorization process may become more complex as it moves from the manual to the online environment: e.g., initials may be keyed into the system by the acquisition department staff but the actual authorizing signature must still appear on the order request. Because of this requirement, auditors often require that these signed order requests be kept as an audit trail.

Two recommendations. Evidence of authorization was one of the primary concerns in the 1987 OSUL audit. Although the primary authorization mechanisms were intact, two recommendations for improvement were made. First, the auditor recommended that a file of the signatures and initials of subject selectors be maintained by the Acquisition Department. These signatures and initials would be used to verify the authorization of each order request.

A second recommendation involved the retrieval and retention of original order request forms submitted by the subject selectors. The auditor's intention was that at the conclusion of the transaction the slips be kept in some organized fashion for three years as proof of authorization. Traditionally, this purchase request form had been used by the Libraries as a processing document which was sent forward with newly received items to cataloging and on to the shelf location with the piece. The auditor viewed this request form as the authorization to purchase while the Libraries viewed the purchase order as the appropriate authorization. Subsequently, the University Archivist, in consultation with the State Auditor, ruled that the request is a processing document and need not be retained. On appeal by Internal Audit, this position was reversed, with a ruling that the request forms were to be retained for one year. As evidenced in this example, librarians should be prepared to negotiate issues where opinions differ.

Recording transactions. Automated systems must be designed in such a way that all transactions are recorded. This will ensure that the financial accounts provide a comprehensive record of each transaction. It is fairly easy for libraries with automated systems to verify that all transactions are recorded through routine comparison of internal accounting records to university accounting reports. However, nonroutine transactions, which occur relatively infrequently and may escape the normal control mechanisms, pose the area of greatest risk. For example, special collection material for unique collections such as cartoon art may not be available through normal channels. Instead, the librarian may purchase material as it is discovered at conferences, exhibits, special sales, etc., and no official purchase request or order is made. Clearly, in order for reimbursement to be made, appropriate documentation must be submitted to the university—therefore, the university requirements in such cases serve as compensating controls. It is imperative, however, that these nonroutine transactions be recreated in the library's internal system sis well as for the university's accounts payable department.

A major consideration in the assessment of internal control is whether the system is effective in filtering out errors and irregularities. The automated system is most effective in the prevention and detection of errors or omissions in recording and entering data, the validation of data, and the rejection of records containing errors. Systems have a number of mechanisms to detect incorrect keying of data. Fixed-length fields have a prescribed number of characters that must be entered, and the data entered must match available codes in the system's internal files. For example, if an order was to be issued on fund "History" but the typist entered "Histroy," the entry would not be accepted and the typist could make corrections. A further control in this area would prohibit the entry of numbers in a field which was limited to alphabetic characters. A loophole in this control is that a system may not be able to identify codes that are generally valid but are used inappropriately.

Systems can be designed to facilitate the data entry process by prompting the typist for the next entry. For example, when orders are entered, a system can automatically move through the fields available for data. At the completion of the entry process, the system can then request the operator to sight verify the data entered. Failing that check, the system can reject the purchase order authorization if essential fields such as fund, location, or vendor are missing. As an added check, the operator can be notified if the receipt date has been omitted when invoices are processed. Finally, systems will invariably detect and note transactions that do not fully offset one another. For example, an account journal entry that transfers money from one fund to another will be verified to determine if the amount debited from one account equals the amount credited to the other account. In the end, financial records are no more accurate than the data entered into the

system. Because almost all data conversion is accomplished by humans and is, therefore, susceptible to error, reliable, accurate controls governing input are particularly important.

Conclusion

Although audits have been a fact of life for many years in libraries, the implementation of automated acquisitions systems has introduced new considerations into the audit process. Internal control mechanisms may be invisible to most library employees, but they cannot be ignored by acquisitions librarians responsible for the process. If internal control mechanisms are carefully planned and documented, if operations are effectively organized with proper segregation of duties, and if employees are competent, well trained, and adequately supervised, the library can confidently prepare for and participate in the organization's internal audit program.

References

1. Wanda A. Wallace, *Handbook of Internal Accounting Controls* (Englewood Cliffs, NJ: Prentice-Hall, 1984), p. 35.
2. Carol E. Chamberlain, "Fiscal Planning in Academic Libraries: The Role of the Automated Acquisitions System," in *Advances in Library Administration and Organization, Vol. 6,* ed. Gerard B. McCabe and Bernard Kreissman (Greenwich, CT: JAI Press, 1986), p. 143.
3. Gorden B. Davis et al., *Auditing and EDP, 2nd* ed. (New York: AICPA, 1983), pp. 6-7.
4. G. Stevenson Smith, *Accounting for Librarians and Other Not-for-Profit Managers.* (Chicago: ALA, 1983), pp. 5-6.
5. 'Jennifer Cargill, "Waiting for the Auditor: Some Interim Advice," *Wilson Library Bulletin* 62 (September 1987): 46-47.
6. 'Robert T. Begg, "Internal Control Systems in the Library Environment," *Journal of Academic Librarianship* 10 (January 1985): 340.
7. Brian Alley and Jennifer Cargill, *Keeping Track of What You Spend: The Librarian's Guide to Simple Bookkeeping* (Phoenix: Oryx, 1982), p. 83.
8. Wallace, *Handbook,* p. 27.
9. 'Howard F. Stettler, *Auditing Principles: A Systems-Based Approach,* 5th ed. (Englewood Cliffs, NJ: Prentice-Hall, 1982), p. 135.
10. Wallace, *Handbook,* pp. 62-63.
11. Stettler, *Auditing Principles,* pp. 255-258.
12. Ibid., p. 123.
13. Begg, "Internal Control Systems," p. 340.
14. Ibid.
15. Wallace, *Handbook,* p. 44.
16. Alley and Cargill, *Keeping Track,* p. 41.
17. Begg, "Internal Control Systems," p. 339.
18. Alley and Cargill, *Keeping Track,* p. 41.